UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/007,859	11/13/2001	Mark C. Astley	GB920010085US1	7123

7590 09/21/2005

IBM Corp, IP Law Dept T81/503
3030 Cornwallis Road
PO Box 12195
Research Triangle Park, NC 27709-2195

EXAMINER
TOLENTINO, RODERICK

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 09/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/007,859	ASTLEY ET AL.	
	Examiner	Art Unit	
	Roderick Tolentino	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09/07/2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 September 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1 – 16 are pending.

Claim Rejections - 35 USC § 112

[001] The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

[002] Claim 4 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

It is unclear as to what the applicant means when stating "using the generated encrypted client password at the client and the stored encrypted client password at the server." It is as best understood by the examiner that the applicant is using the encrypted passwords to create a shared secret session key.

Claim Rejections - 35 USC § 102

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

[003] Claims 1 – 3, 6 – 8 and 12 - 16 are rejected under 35 U.S.C. 102(b) as being anticipated by Davis et al. U.S. Patent No. (6,064,736).

[004] As per claim 1 Davis teaches a process at the client data processing system applying the cipher function to the client password, which corresponds to the stored cipher-protected client password, thereby to generate a cipher-

protected client password, which is equivalent to the stored cipher-protected client password; (Davis, Fig.3, Item 321, Client hashes password) and performing an authentication check using the client data processing system's cipher-protected client password and the server data processing system's stored cipher-protected client password as a shared secret for said authentication check (Davis, Fig. 3, Col. 4 Lines 42 – 56).

[005] As per claim 2 Davis teaches an authentication check includes performing a mutual challenge-response authentication protocol check (Davis, Fig. 3, Items 319, 321, 323, 327, 329, 331 and 333).

[006] As per claim 3 Davis teaches the cipher function is an encryption algorithm (Davis, Col. 4, Lines 50 – 52).

[007] As per claim 6 Davis teaches the cipher function is a hash function (Davis, Col. 4, Lines 50 – 52).

[008] As per claim 7 Davis discloses a process at the server data processing system retrieving from the repository the respective token for a stored cipher-protected client password, and transmitting the token to a client data processing system (Davis, Col. 5, Lines 11 – 14) and the process at the client data processing system applying the cipher function to the combination of the transmitted token and the client password which corresponds to the stored cipher-protected client password, thereby to generate the equivalent cipher-protected client password for use as a shared secret (Davis, Col. 5, Lines 18 – 31).

[009] As per claim 8 Davis discloses the token is a random number (Davis, Col. 5, Lines 11 – 13, salt).

[010] As per claims 12 - 15 Davis discloses a process at the server data processing system retrieving from the repository the respective token for a stored cipher-protected client password (Davis, Fig 5 Item 311), and transmitting the token to a client data processing system (Davis, Col. 5, Lines 11 - 20), a process at the client data processing system applying the cipher function to the combination of the transmitted token and the client password which corresponds to the stored cipher-protected client password (Davis, Col. 5 Lines 23- 24), thereby to generate a cipher-protected client password which is equivalent to the stored cipher-protected client password (Davis, Fig. 5 Item 521), and using the client data processing system's cipher-protected client password and the server data processing system's stored cipher-protected client password as a shared secret for a mutual challenge-response authentication check (Davis, Fig. 5 Items 327, 329, 531, 333 and 335).

[011] As per claim 16 Davis discloses generating a cipher-protected client password by applying said first cipher function to the client's password, thereby to provide the client and server processes with a shared secret (Davis, Col. 5 Lines 11 –13), generating a client response and counter-challenge to the server challenge, the client response and counter-challenge including a message authentication code computed using the cipher-protected client password (Davis, Fig. 5, Items 521 and 523), forwarding the client response and counter-challenge to the server process (Davis, Fig. 5, Item 329) receiving the forwarded server

response; generating an anticipated server response and comparing the received and anticipated server responses to determine whether they match; and in response to a positive match, confirming successful authentication (Davis. Fig. 5, Items 531, 533 and 335).

Claim Rejections - 35 USC § 103

[012] The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

[013] Claim 4, 5, 9,10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al. U.S. Patent No. (6,064,736) in view of Yatsukawa U.S. Patent No. (6,148,404).

[014] As per claim 4 Davis fails to disclose an authentication check comprises generating a common secret session key at both the client and server data processing systems, using the generated encrypted client password at the client and the stored encrypted client password at the server, and using this common secret session key in a mutual challenge-response authentication protocol. However, Yatsukawa discloses an authentication check comprises generating a common secret session key at both the client and server data processing systems, using the generated encrypted client password at the client and the stored encrypted client password at the server, and using this common secret

session key in a mutual challenge-response authentication protocol (Yatsukawa, Col. 19, Lines 62 – 67).

[015] At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to us a common session-key with Davis' password verification method and system, because it offers the advantage of confidentiality by limiting the chance of leakage of information between client and server along with unauthorized intrusion (Yatsukawa, Col. 1 Lines 35 – 42).

[016] As per claim 5 Davis as modified discloses a secret session key is generated by applying a cipher function to each of the generated encrypted client password at the client and the stored encrypted client password at the server (Col. 3, Lines 52 – 55).

[017] As per claim 9 Davis fails to disclose the server processing system's password repository is preferably integrated within the operating system of the server data processing system. However, Yatsukawa discloses the server processing system's password repository is preferably integrated within the operating system of the server data processing system (Yatsukawa, Col. 19, Lines 1 – 6).

[018] At the time the invention was made it would have been obvious to a person of ordinary skill in the art to use an operating system with Davis' password verification method and system, because it offers the advantage of increasing the confidentiality and integrity to a system. (Yatsukawa, Col. 1, Lines 33 - 38).

[019] As per claim 10 Davis as modified discloses the operating system is an operating system conforming to the UNIX operating system standard or derived from a UNIX conforming system (Yatsukawa, Col. 19, Lines 3 – 6).

[020] As per claim 11 Davis discloses the encryption algorithm is provided by the UNIX crypt() function (Davis, Col. 5, Lines 13 – 16).

Conclusion

[021] Any inquiry concerning this communication or earlier communications from the examiner should be directed to Roderick Tolentino whose telephone number is (571) 272-2661. The examiner can normally be reached on 8:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Roderick Tolentino

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100